

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for providing automated diagnosis of problems for a computer network, comprising:

receiving input regarding a problem with the computer network;

identifying recent configuration changes made to the computer network that are associated with parameters of the problem fall within pre-established parameters;

associating each of the identified configuration changes with a rank based on a likelihood that each of the identified configuration changes caused the problem; and ranking the identified changes into potential causes;

verifying that the ranked potential causes configuration changes are related to the problem to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem; and

calculating distances associated with the ranked potential causes that correspond to a relative likelihood that potential causes may be a true cause.

2. (Currently Amended) The method of ~~claim 1~~ claim 7, further comprising:

formulating a list of possible causes the configuration changes based on or ordered in terms of the distances adjusted rank associated with each of the verified configuration changes; and

presenting the list to a user.

3. (Currently Amended) The method of ~~claim 1~~ claim 7, further comprising:

comparing the determined distance associated with each of the verified configuration changes with a configurable distance threshold; and

discarding any of the verified configuration changes associated with the determined distance that violates the configurable distance threshold ranked potential causes that violate a configurable distance threshold.

4. (Currently Amended) The method of claim 1, further comprising:

recording ~~policy or the~~ configuration changes ~~that occur~~ made to the computer network; and

in response to receiving the input regarding the problem, recording the configuration changes associated with the problem at an adjusted level of detail.

5. (Currently Amended) The method of claim 1, further comprising accumulating ~~and ranking potential causes until all potential causes~~ and filtering the received input associated with the problem until all of the input is ~~are~~ received.

6. (Currently Amended) The method of claim 1, further comprising searching a database having user records, vulnerability and reliability data to verify the ~~potential causes~~ ranked configuration changes.

7. (Currently Amended) The method of claim 1, further comprising:
~~interpreting the computer network's policies as needed to complete the verifying step~~ determining a distance between each of the verified configuration changes and the problem;
and

adjusting the rank associated with each of the verified configuration changes based on the determined distance between each of the verified configuration changes and the problem.

8. (Currently Amended) A computer-readable medium executable on a computer having a program for providing automated diagnosis of problems for a computer network, ~~for performing the steps of~~ comprising:

logic configured to receive input regarding a problem with the computer network;

logic configured to identify ~~recent~~ configuration changes made to the computer network that are associated with parameters of the problem ~~fall within pre-established parameters;~~

logic configured to ~~rank the identified changes into potential causes~~ associate each of the identified configuration changes with a rank based on a likelihood that each of the identified configuration changes caused the problem; and

logic configured to verify that the ranked potential causes configuration changes are related to the problem ~~to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem;~~ and

~~logic configured to calculate distances associated with the ranked potential causes that correspond to a relative likelihood that potential causes may be a true cause.~~

9. (Currently Amended) The computer-readable medium of ~~claim 8~~ claim 10, further comprising:

logic configured to formulate a list of ~~possible causes~~ the configuration changes based on the ~~distances~~ adjusted rank associated with each of the verified configuration changes; and

logic configured to present the list to a user.

10. (Currently Amended) The computer-readable medium of claim 8, further comprising:

logic configured to determine a distance between each of the verified configuration changes and the problem; and

logic configured to adjust the rank associated with each of the verified configuration changes based on the determined distance between each of the verified configuration changes and the problem

~~logic configured to discard the ranked potential causes that violate a configurable distance threshold.~~

11. (Currently Amended) The computer-readable medium of claim 8, further comprising:

logic configured to record ~~policy or the~~ configuration changes that occur made to the computer network; and

logic configured to record the configuration changes associated with the problem at an adjusted level of detail in response to receiving the input regarding the problem.

12. (Currently Amended) The computer-readable medium of claim 8, further comprising logic configured to accumulate and ~~rank the potential causes~~ filter the received input associated with the problem until all ~~potential causes associated with the problem are of the input is~~ received.

13. (Currently Amended) The computer-readable medium of claim 8, further comprising logic configured to search a database having user records, vulnerability and reliability data to verify the ~~potential causes~~ ranked configuration changes.

14. (Currently Amended) A system for providing automated diagnosis of problems for a computer network, comprising:

~~a central diagnosis engine configured to include:~~

means operative to receive input regarding a problem with the computer network;

means operative to identify configuration changes made to the computer network that are associated with parameters of the problem;

~~a rank estimator module configured~~ means operative to associate each of the identified configuration changes with a rank identified changes into potential changes based on a likelihood that each of the identified configuration changes caused the problem; and

~~a verifier module configured~~ means operative to verify that the ranked potential causes configuration changes are related to the problem to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem; and

~~a distance estimator module configured to calculate distances associated with the ranked potential causes that correspond to a relative likelihood that potential causes may be a true cause; and~~

~~an adaptive logger operative coupled to the central diagnosis engine, the adaptive logger is configured to record policy or configuration changes made to the computer network that fall within pre-established parameters.~~

15. (Currently Amended) The system of claim 14, further comprising ~~an input parser/filter module operatively coupled to the central diagnosis engine, the input parser/filter including logic configured~~ means operative to receive policy or profile input from a user's

processing device or policy-management systems and to convert the policy or profile input into data usable by the central diagnosis engine usable data.

16. (Currently Amended) The system of claim 14, further comprising: ~~an input parser/filter module operatively coupled to the central diagnosis engine, the input parser/filter including logic configured to receive a problem indication and descriptive information from sensor and monitoring systems and to convert that input into data usable by the central diagnosis engine~~

means operative to determine a distance between each of the verified configuration changes and the problem; and

means operative to adjust the rank associated with each of the verified configuration changes based on the determined distance between each of the verified configuration changes and the problem.

17. (Currently Amended) The system of ~~claim 15~~ claim 14, further comprising a database populated with descriptive system information and a database structure configured as hierarchical database pages, each database page having a page index, data section and selector section, ~~and~~ wherein the data section is further configured to include ~~the element~~ reliability or vulnerability information associated with an element of the computer network associated with the problem, and wherein the selector section is further configured to include links to related database pages.

18. (Currently Amended) The system of ~~claim 17~~ claim 14, ~~wherein the central diagnosis engine further comprises a problem accumulator module configured~~ further comprising means operative to receive problem data from the input parser/filter module and to continue receive data accumulate and filter the received input regarding the problem with the computer network until the problem is fully described all of the input is received.

19. (Currently Amended) The system of ~~claim 18~~ claim 14, wherein ~~the central diagnosis engine further comprises a cause estimator module configured to interface with the adaptive logger and to identify any changes in policy or configuration associated with any~~

~~available parameters of the problem~~ the parameters of the problem include at least one of an element of the computer network experiencing the problem, an element of the computer network affected by the problem, and a time at which the problem was first noted.

20. (Currently Amended) ~~The system of claim 19, wherein the central diagnosis engine further comprises a possible cause accumulator module configured to receive and accumulate potential causes and rankings from the rank estimator module until the ranking is complete and potential causes associated with the problem are received~~ The method of claim 1, wherein the parameters of the problem include at least one of an element of the computer network experiencing the problem, an element of the computer network affected by the problem, and a time at which the problem was first noted.

21. (Currently Amended) ~~The system of claim 20, wherein the central diagnosis engine further comprises a policy interpreter module configured to provide details on the computer network's configuration to the verifier module as needed in the verification process~~ The computer-readable medium of claim 8, wherein the parameters of the problem include at least one of an element of the computer network experiencing the problem, an element of the computer network affected by the problem, and a time at which the problem was first noted.

22. (Currently Amended) ~~The system of ~~claim 21~~ claim 16, further comprising: a presentation module operatively coupled to the central diagnosis engine and a user's processing device through a communications network, the presentation module configured to summarize and format at least one of accumulated possible causes, distances, probabilities, related reliability or vulnerability results for utilization by the user's processing device~~

means operative to formulate a list of the configuration changes based on the adjusted rank associated with each of the verified configuration changes; and

means operative to present the list to a user.

23. (Currently Amended) ~~The system of ~~claim 22~~ claim 17, further comprising a database interface module operatively coupled between the database, the database structure, and~~

~~the central diagnosis engine, the database interface module configured~~ means operative to enable provisioning and access to the database and the database structure.

24. (Currently Amended) The system of ~~claim 23~~ claim 17, wherein the database comprises an element descriptive database (EDD).

25. (Currently Amended) The system of ~~claim 24~~ claim 17, wherein the database structure comprises a hierarchical vulnerability database (HVD) structure.